Notice of Allowability	Application No.	Applicant(s)	
	10/719,836	GOULD, KENNETH	
	Examiner	Art Unit	
	MICHAEL J. SIMITOSKI	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the repsonse of 5/20/2008*.

2. ☒ The allowed claim(s) is/are *7-28,36-48,52 and 53*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date See Continuation Sheet
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20080730* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Continuation of Attachment(s) 3. Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date: 7/23/07, 7/18/07, 11/8/04.

DETAILED ACTION

1. The response of 5/20/2008 was received and considered.

2. Claims 7-28, 36-48 & 52-53 are pending.

Inventorship

3. In view of the papers filed 12/21/2007, it has been found that this nonprovisional application, as filed, through error and without deceptive intent, improperly set forth the inventorship, and accordingly, this application has been corrected in compliance with 37 CFR 1.48(a). The inventorship of this application has been changed by addition of inventor Christopher Pierce Williams as a co-inventor.

The application will be forwarded to the Office of Initial Patent Examination (OIPE) for issuance of a corrected filing receipt, and correction of Office records to reflect the inventorship as corrected.

Election/Restrictions

4. Claims 7-28, 36-48 & 52-53 are allowable. The restriction requirement between species, as set forth in the Office action mailed on 5/9/2008, has been reconsidered in view of the allowability of claims to the elected invention pursuant to MPEP § 821.04(a). **The restriction requirement is hereby withdrawn as to any claim that requires all the limitations of an allowable claim.** Claims 8-9, 13-14, 18-19, 24-25, 39-40 & 45-46, directed to species AI and AII are no longer withdrawn from consideration because the claim(s) requires all the limitations of an allowable claim.

5. In view of the above noted withdrawal of the restriction requirement, applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

Once a restriction requirement is withdrawn, the provisions of 35 U.S.C. 121 are no longer applicable. See *In re Ziegler*, 443 F.2d 1211, 1215, 170 USPQ 129, 131-32 (CCPA 1971). See also MPEP § 804.01.

EXAMINER'S AMENDMENT

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Elliot Light on 7/30/2008.

The application has been amended as follows:

Please **REPLACE** the **CURRENT CLAIM LISTING** with the **FOLLOWING**:

1-6 (Canceled)

7. (Currently Amended) A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD) comprising:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to the cable system and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address;

comparing components of proffered identifier to the components of each of one or more stored identifiers stored in a datastore;

making a determination whether the proffered identifier and any of the one or more stored identifiers satisfy a matching criteria comprising a same CMAD MAC address component and a different gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the matching criteria, selecting a remedial response, wherein the remedial response comprises denying the CMAD access to the cable system.

8. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the datastore comprises a central database.

9. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the datastore comprises a distributed database.

10. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the cable system comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the determination with respect to the matching criteria.

11. (Currently Amended) The method for detecting unauthorized access of a cable system by a CMAD of claim 7, wherein the remedial response further comprises, sending an advisory message to a network manager and recording an event in a log file.

12. (Currently Amended) A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD) comprising:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to the cable system and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address;

comparing components of the proffered identifier to components of each of one or more stored identifiers stored in a datastore;

making a determination whether the proffered identifier and any of the one or more stored identifiers satisfies a matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the matching criteria, selecting a remedial response, wherein the remedial response comprises denying the CMAD access to the cable system.

13. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the datastore comprises a central database.

14. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the datastore comprises a distributed database.

15. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the cable system further comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the determination with respect to the matching criteria.

16. (Currently Amended) The method for detecting unauthorized access of a cable system by a CMAD of claim 12, wherein the remedial response further comprises sending an advisory message to a network manager and recording an event in a log file.

17. (Currently Amended) A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD) comprising:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to the cable system and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address;

comparing components of the proffered identifier to components of each of one or more stored identifiers stored in a datastore;

making a first determination whether the proffered identifier and any of the one or more stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component;

in the event the proffered identifier and any of the one or more stored identifiers satisfy the first matching criteria, selecting a first remedial response, wherein the first remedial response comprises denying the CMAD access to the cable system;

in the event the proffered identifier and any of the one or more stored identifiers do not satisfy the first matching criteria, making a second determination whether the proffered identifier and any of the one or more stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the second matching criteria, selecting a second remedial response, wherein the second remedial response comprises denying the CMAD access to the cable system.

18. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the datastore comprises a central database.

19. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the datastore comprises a distributed database.

20. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the cable system further comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the determination with respect to the first matching criteria and the determination with respect to the second matching criteria.

21. (Currently Amended) The method for detecting unauthorized access of a cable system by a CMAD of claim 17, wherein the remedial responses further comprise sending an advisory message to a network manager and recording an event in a log file.

22. (Currently Amended) The method for detecting unauthorized access of a cable system by a CMAD of claim 17, further comprising in the event that the proffered identifier and any of the one or more stored identifiers do not satisfy the first matching criteria and the second matching criteria, storing the proffered identifier in the datastore.

23. (Currently Amended) A method for detecting unauthorized access of a cable system by a cable modem auxiliary device (CMAD), wherein the cable system comprises a plurality of regional cable networks each having a regional datastore, the method comprising:

receiving at a cable modem termination system (CMTS) a DHCP request comprising a MAC address of a CMAD seeking access to the cable system through one of the plurality of regional cable networks and a MAC address of a cable modem (CM) to which the CMAD is connected;

forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address;

comparing components of the proffered identifier to components of each of one or more regionally stored identifiers stored in a regional datastore;

making a first determination whether the proffered identifier and any of the one or more regionally stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the matching criteria, selecting a first remedial response, wherein the first remedial response comprises denying the CMAD access to the cable system;

in the event the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria, making a second determination whether the proffered identifier and any of the one or more regionally stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the second matching criteria, selecting a second remedial response, wherein the second remedial response comprises denying the CMAD access to the cable system;

in the event that the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria and the second matching criteria, comparing components of the proffered identifier to components of each of one or more centrally stored identifiers stored in a central datastore, wherein the central datastore comprises regionally stored identifiers from each of the regional datastores;

making a third determination whether the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria;

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria, selecting a third remedial response, wherein the third remedial response comprises denying the CMAD access to the cable system;

in the event the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching criteria, making a fourth determination whether the proffered identifier and any of the one or more centrally stored identifiers satisfies the second matching criteria; and

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the second matching criteria, selecting a fourth remedial response, wherein the fourth remedial response comprises denying the CMAD access to the cable system.

24. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the regional datastore and the central datastore each comprise a central database.

25. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the regional datastore and the central datastore each comprise a distributed database.

26. (Original) The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the one of the plurality of regional cable networks through which access to the cable system is sought further comprises a DHCP server linked to the CMTS and wherein the DHCP server makes the first determination and the second determination.

27. (Currently Amended) The method for detecting unauthorized access of a cable system by a CMAD of claim 23, wherein the remedial responses further comprise sending an advisory message to a network manager and recording an event in a log file.

28. (Currently Amended) The method for detecting unauthorized access of a cable system by a CMAD of claim 23, further comprising in the event that the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching

criteria and the second matching criteria, storing the proffered identifier in the regional datastore and the central datastore.

29-35. (Canceled)

36. (Currently Amended) A system for detecting unauthorized access of a cable network by a cable modem auxiliary device (CMAD) comprising:

a CMAD seeking access to the cable network;

a CMTS, wherein the CMTS is configured for:

receiving a DHCP request comprising a MAC address of the CMAD seeking access to the cable network and a MAC address of a cable modem (CM) to which the CMAD is connected; and

forming a proffered identifier by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address; and

a detection server linked to a datastore, wherein the detection server is configured for:

receiving the proffered identifier from the CMTS;

comparing components of the proffered identifier to components of each of one or more stored identifiers stored in the datastore;

determining whether the proffered identifier and any of the one or more stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the first matching criteria, selecting a remedial response, wherein the remedial response comprises denying the CMAD access to the cable network.

37. (Currently Amended) The system of claim 36, wherein the detection server is further configured for:

determining whether the proffered identifier and any of the one or more stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component; and

in the event the proffered identifier and any of the one or more stored identifiers satisfy the second matching criteria, selecting a second remedial response, wherein the second remedial response comprises denying the CMAD access to the cable network.

38. (Currently Amended) The system of claim 37, wherein the detection server is further configured for in the event the proffered identifier and any of the one or more stored identifiers do not satisfy the first matching criteria and the second matching criteria, storing the proffered identifier in the datastore.

39. (Original) The system of claim 36, wherein the datastore comprises a central database.

40. (Original) The system of claim 36, wherein the datastore comprises a distributed database.

41. (Original) The system of claim 36, wherein the remedial response comprises denying the CMAD access to the cable network, sending an advisory message to a network manager, and recording an event in a log file.

42. (Original) The system of claim 36, wherein the detection server comprises a DHCP server.

43. (Currently Amended) A system for detecting unauthorized access of a cable system comprising a plurality of regional cable networks by a cable modem auxiliary device (CMAD), the system comprising:

a CMAD seeking access to the cable system through one of the plurality of regional cable networks;

a CMTS, wherein the CMTS is configured for:

receiving a DHCP request comprising a MAC address of the CMAD seeking access to one of the plurality of regional cable networks and a MAC address of a cable modem (CM) to which the CMAD is connected; and

forming a proffered identifier by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address; and

a regional detection server linked to a regional datastore, wherein the regional detection server is configured for:

receiving the proffered identifier from the CMTS;

comparing components of the proffered identifier to components of each of one or more regionally stored identifiers stored in the regional datastore;

determining whether the proffered identifier and any of the one or more regionally stored identifiers satisfy a first matching criteria comprising a same CMAD MAC address component and a different gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the first matching criteria, selecting a first remedial response, wherein the first remedial response comprises denying the CMAD access to the cable system;

in the event the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria, determining whether the proffered identifier and any of the one or more regionally stored identifiers satisfies a second matching criteria comprising a same CMAD MAC address component, a different CM MAC address component, and a same gateway interface address component;

in the event the proffered identifier and any of the one or more regionally stored identifiers satisfy the second matching criteria, selecting a second remedial response, wherein the second remedial response comprises denying the CMAD access to the cable system;

in the event that the proffered identifier and any of the one or more regionally stored identifiers do not satisfy the first matching criteria and the second matching criteria, sending the proffered identifier to a central detection server; and

the central detection server linked to a central datastore, the central detection server configured for:

comparing components of the proffered identifier to components of each of one or more centrally stored identifiers stored in a central datastore, wherein the central datastore comprises regionally stored identifiers from each of the regional datastores;

determining whether the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria;

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the first matching criteria, selecting a third remedial response;

in the event the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching criteria, determining whether the proffered identifier and any of the one or more centrally stored identifiers satisfies the second matching criteria; and

in the event the proffered identifier and any of the one or more centrally stored identifiers satisfy the second matching criteria, selecting a fourth remedial response, wherein the fourth remedial response comprises denying the CMAD access to the cable system.

44. (Currently Amended) The system of claim 43, wherein the central detection server is further configured for in the event the proffered identifier and any of the one or more centrally stored identifiers do not satisfy the first matching criteria and the second matching criteria, storing the proffered identifier in the regional datastore and the central datastore.

45. (Original) The system of claim 43, wherein the regional datastore and the central datastore each comprise a central database.

46. (Original) The system of claim 43, wherein the regional datastore and the central datastore each comprise a distributed database.

47. (Currently Amended) The system of claim 43, wherein the remedial responses further comprise sending an advisory message to a network manager and recording an event in a log file.

48. (Original) The system of claim 43, wherein the regional detection server comprises a DHCP server.

49-51. (Canceled)

52. (New) The method for detecting unauthorized access of a cable system by a CMAD of claim 7 further comprising in the event that the proffered identifier and any of the one or more stored identifiers do not satisfy the matching criteria, storing the proffered identifier in the datastore.

53. (New) The method for detecting unauthorized access of a cable system by a CMAD of claim 12 further comprising in the event that the proffered identifier and any of the one or more stored identifiers do not satisfy the matching criteria, storing the proffered identifier in the datastore.

Allowable Subject Matter

7. The following is an examiner's statement of reasons for allowance:

a. The reference to Sawyer et al. teaches recording a CM MAC address, a STB IP address and a STB MAC address, where the CM MAC address is "tagged" to a field in a DHCP packet (at least cols. 3-4).

b. The reference to Schmuelling et al. reference teaches comparing a MAC address of a cable modem to a database to determine if the modem is an established modem of an ISP (at least col. 3) in combination with DHCP.

c. The reference to Beser et al. teaches a CM and a CMTS storing ARP tables (in accordance with DHCP) where the tables contain MAC address/IP address pairs of the CPE and CM, respectively.

d. The reference to Kumar teaches determining if a router (gateway) exists between a customer premise equipment and a cable modem in a DOCSIS system by using ARP tables.

e. The reference to Lui teaches a MAC management unit to determine if a destination address provided in a packet matches a network address of a cable modem or CPE and if it does not match, rejecting the packet; if a match exists, a cable modem determines whether the address corresponds to the cable modem (at least col. 9).

f. The reference to Bahlmann teaches controlling a cable network through ARP tables and MAC addresses.

g. The reference to Chien et al. teaches monitoring traffic, determining if a device was the first to be assigned an IP address and allowing or denying traffic based on confirming or denying the determination (at least p. 3).

h. The reference to Garrett et al. teaches comparing a source IP address in a packet header to a list of addresses allocated to subscribers of services and denying a packet accordingly if there is no match (at least p. 3).

i. The reference to Massarani teaches the use of DHCP and ARP to control security breaches in a network by comparing an end user MAC address with a database of valid addresses (at least col. 3).

j. The reference to Willming et al. teaches using digital certificates in combination with DHCP to control access to a cable network.

k. The reference to Lim et al. teaches using a secure DHCP server where DHCP renewal is contingent upon factors such as the number of requests/leases.

l. The reference to Jones et al. (RFC 3256) teaches DHCP relay agent information as it relates to DOCSIS (adding device class information).

m. The reference to Thomson et al. (RFC 2462) is cited for teaching how to configure hosts in IPv6.

n. The reference to Patrick (RFC 3046) teaches using DHCP with a cable system.

o. The Williams et al. reference is the published patent of a related application to the instant application, with same inventors.

8. However, regarding claims 7, 12, 17, 23, 36 & 43, the prior art of record, either alone or in combination, fails to teach receiving, at a cable modem termination system (CMTS), a DHCP request comprising a MAC address of a cable modem auxiliary device (CMAD) seeking access to a cable system and a MAC address of a cable modem (CM) to which the CMAD is connected, forming a proffered identifier of the CMAD by combining a gateway interface address of the CMTS with the CM MAC address and the CMAD MAC address, comparing the proffered identifier to stored identifiers in a database, determining if the proffered identifier and the stored identifiers satisfy a matching criteria comprising a same CMAD AMC address and a different gateway interface address and if the matching criteria is satisfied, denying access to the system, in combination with the remaining elements of the claims as a whole, and as disclosed on at least pp. 2-4 & 17-22 of the specification.

Claims 8-11, 13-16, 18-22, 24-28, 37-42, 44-48 & 52-53 are allowable based on their dependence upon an allowed claim.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

July 30, 2008
/Michael J Simitoski/
Primary Examiner, Art Unit 2134